

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**

Docket No. 208915US2RD/vdm

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Masahiro TAKAGI, et al.

GAU: 2661

SERIAL NO: 09/862,440

EXAMINER:

FILED: May 23, 2001

FOR: COMMUNICATION CONTROL SCHEME USING PROXY DEVICE AND SECURITY PROTOCOL COMBINATION

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number [US App No], filed [US App Dt], is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date of U.S. Provisional Application Serial Number, filed, is claimed pursuant to the provisions of 35 U.S.C. §119(e).
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
JAPAN	2000-151434	May 23, 2000

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number .
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
(B) Application Serial No.(s)
 - ☐ are submitted herewith
 - ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Joseph A. Scafetta Jr.
Marvin J. Spivak

Registration No. 24,913

Joseph A. Scafetta, Jr.
Registration No. 26,803



22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)



日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年 5月23日

出 願 番 号

Application Number:

特願2000-151434

出 願 人

Applicant(s):

株式会社東芝

RECEIVED
SEP 18 2001
Technology Center 2600

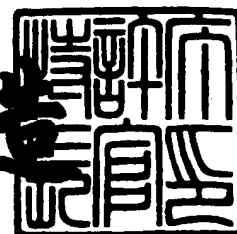
RECEIVED
OCT 19 2001
Technology Center 2100

RECEIVED
OCT 23 2001
Technology Center 2600

2001年 5月30日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3047416

【書類名】 特許願

【整理番号】 13B0050291

【提出日】 平成12年 5月23日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/66
H04B 7/26
H04Q 7/22

【発明の名称】 ゲートウェイ装置、通信装置、制御装置、および通信制御方法

【請求項の数】 12

【発明者】
【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝
研究開発センター内
【氏名】 高木 雅裕

【発明者】
【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝
研究開発センター内
【氏名】 石山 政浩

【特許出願人】
【識別番号】 000003078
【氏名又は名称】 株式会社 東芝

【代理人】
【識別番号】 100081732
【弁理士】
【氏名又は名称】 大胡 典夫

【選任した代理人】
【識別番号】 100075683
【弁理士】
【氏名又は名称】 竹花 喜久男

【選任した代理人】

【識別番号】 100084515

【弁理士】

【氏名又は名称】 宇治 弘

【手数料の表示】

【予納台帳番号】 009427

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0001435

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ゲートウェイ装置、通信装置、制御装置、および通信制御方法

【特許請求の範囲】

【請求項 1】

無線網に収容された無線端末装置と有線網に収容された有線端末装置との間で
トランスポート層以上の情報の中継を行うゲートウェイ装置において、

前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために、
前記無線端末装置と前記有線端末装置との間に設定される第 1 のセキュリティ
アソシエーションに関する情報を保持する第 1 のセキュリティ情報保持手段と、

前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信を中継す
る際に前記第 1 セキュリティアソシエーションに関する情報を利用して前記無線
端末装置もしくは前記有線端末装置に受信される暗号化された情報を復号化する
情報復号化手段と、

前記復号化された情報に基づいて前記トランスポート層以上の情報を利用して
中継処理を行う中継手段と、

前記中継手段が送信する情報を前記第 1 のセキュリティアソシエーションに関
する情報を利用して秘匿化する情報暗号化手段と
を具備したことを特徴とするゲートウェイ装置。

【請求項 2】

無線網に収容された無線端末装置と有線網に収容された有線端末装置との間で
トランスポート層以上の情報の中継を行うゲートウェイ装置において、

前記無線端末装置と前記有線端末装置との間で情報の認証を保証した通信を行
うために、前記無線端末装置と前記有線端末装置との間に設定される第 1 のセキ
ュリティアソシエーションに関する情報を保持する第 1 のセキュリティ情報保持
手段と、

前記無線端末装置と前記有線端末装置との間で前記認証を保証された情報を前
記トランスポート層以上の情報を利用して中継処理を行う中継手段と、

前記中継手段が中継する前記認証が保証された情報および前記中継手段が必要
に応じて新たに生成した情報に対して前記第 1 のセキュリティアソシエーション

に関する情報を利用して、前記認証が保証された情報を保証する認証情報を付加する認証情報手段と

を具備したことを特徴とするゲートウェイ装置。

【請求項 3】

無線網に収容された無線端末装置もしくは有線網に収容された有線端末装置のいずれかに設けられ、

前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第 1 のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第 2 のセキュリティアソシエーションに関する情報を、前記無線端末装置と前記有線端末装置との間でトランスポート層以上の情報を用いた中継を行うゲートウェイ装置に提供するセキュリティ情報提供手段を具備したことを特徴とする通信装置。

【請求項 4】

前記第 1 乃至前記第 2 のセキュリティアソシエーションに関する情報は、前記無線端末装置と前記有線端末装置との間でトランスポート層以上の情報の通信を行う際に前記情報のセキュリティを管理するセキュリティサーバから前記ゲートウェイ装置に提供されることを特徴とする請求項 3 に記載の通信装置。

【請求項 5】

無線網に収容された無線端末装置と有線網に収容された有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第 1 のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第 2 のセキュリティアソシエーションに関する情報を生成するセキュリティ情報生成手段と、

前記生成された第 1 乃至第 2 のセキュリティアソシエーションを前記無線端末装置乃至前記有線端末装置に配布するセキュリティ情報配布手段とを具備したことを特徴とする制御装置。

【請求項 6】

無線網に收容された無線端末装置と有線網に收容された有線端末装置との間で
トランスポート層以上の情報の中継の制御を行う制御装置において、

前記無線端末装置と前記有線端末装置に設けられた検索鍵に対する、前記無線
端末装置乃至前記有線端末装置に設けられた検索鍵に対して、前記無線端末装置
と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と
前記有線端末装置との間に設定される第 1 のセキュリティアソシエーションに関
する情報、乃至前記無線端末装置と前記有線端末装置との間で前記情報の認証を
保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定さ
れる第 2 のセキュリティアソシエーションに関する情報を検索し抽出するセキュ
リティ情報検索手段を具備したことを特徴とする制御装置。

【請求項 7】

無線網に收容された無線端末装置と有線網に收容された有線端末装置との間で
トランスポート層以上の情報の中継を行う通信装置において、

前記情報の内容に基づいて前記無線端末装置と前記有線端末装置との間で中継
処理を行う中継手段を動作させるか否かを選択し、

前記中継手段を動作させる場合には前記無線端末装置と前記有線端末装置との
間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間
に設定される第 1 のセキュリティアソシエーションに関する情報、乃至前記無線
端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うため
に前記無線端末装置と前記有線端末装置との間に設定される第 2 のセキュリティ
アソシエーションに関する情報を用いて通信を行い、

前記中継手段を動作させない場合には前記無線端末装置と前記有線端末装置と
の間で通信を行うための第 3 のセキュリティアソシエーションに関する情報を設
定し通信を行わせる選択手段を具備したことを特徴とする通信装置。

【請求項 8】

無線網に收容された無線端末装置と有線網に收容された有線端末装置との間で
ゲートウェイ装置を介してトランスポート層以上の情報の中継を行う通信制御方
法において、

第1のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第1のセキュリティアソシエーションに関する情報、乃至前記第1のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第2のセキュリティアソシエーションに関する情報を、第2のゲートウェイ装置に引き渡す工程と、

前記無線端末装置と前記有線端末装置との間の前記秘匿性乃至前記認証を保証した通信が、前記第1のゲートウェイ装置から前記第2のゲートウェイ装置に変化して経由された場合に、前記第1のゲートウェイ装置で行っていた前記トランスポート層以上の情報を利用した中継処理を前記引き渡された第1及び第2のセキュリティアソシエーションに関する情報を利用して前記第2のゲートウェイ装置において動作される工程とを有することを特徴とする通信制御方法。

【請求項9】

無線網に收容された無線端末装置と有線網に收容された有線端末装置との間でゲートウェイ装置を介してトランスポート層以上の情報の中継を行う通信制御方法において、

第1のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第1のセキュリティアソシエーションに関する情報、乃至前記第1のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第2のセキュリティアソシエーションに関する情報を、第2のゲートウェイ装置に引き渡す工程と、

前記無線端末装置と前記有線端末装置との間の前記秘匿性乃至前記認証を保証した通信が、前記第1のゲートウェイ装置から前記第2のゲートウェイ装置に変化して経由された場合に、前記第1のゲートウェイ装置で行っていた前記トランスポート層以上の情報を利用した中継処理を前記引き渡された第1及び第2のセ

セキュリティアソシエーションに関する情報及び前記トランスポート層以上の状態を利用して前記第 2 のゲートウェイ装置において動作される工程とを有することを特徴とする通信制御方法。

【請求項 1 0】

無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継を行うゲートウェイ装置において、

第 1 のゲートウェイ装置を通過した前記情報をカプセル化する第 2 のゲートウェイ装置と、

前記カプセル化された情報からカプセルを取り除き、前記カプセルが取り除かれた情報を前記トランスポート層以上の情報を利用して中継を行う必要があるかを判断し、必要な場合には中継を行う第 3 のゲートウェイ装置と、

前記第 3 のゲートウェイ装置から送られた情報をカプセル化するカプセル化手段と

を具備したことを特徴とするゲートウェイ装置。

【請求項 1 1】

ネットワークによって相互に通信可能な第 1 の通信装置と第 2 の通信装置との間で、トランスポート層以上の情報を利用した中継を行なうゲートウェイ装置において、

前記第 1 の通信装置と第 2 の通信装置との間で秘匿性を保証する通信のために、前記第 1 の通信装置と第 2 の通信装置との間に設定される第 1 のセキュリティアソシエーションに関する情報を保持する第 1 のセキュリティ情報保持手段と、

前記第 1 の通信装置と第 2 の通信装置との間で秘匿性を保証する通信を中継する際に前記第 1 のセキュリティアソシエーションに関する情報を利用して、前記第 2 の通信装置もしくは第 2 の通信装置に受信される暗号化された情報を復号化する情報復号化手段と、

前記復号化された情報に基づいて前記トランスポート層以上の情報を利用して中継処理を行う中継手段と、

前記中継手段が送信する情報を前記第 1 のセキュリティアソシエーションに関する情報を利用して秘匿化する情報暗号化手段と

を具備したことを特徴とするゲートウェイ装置。

【請求項 1 2】

ネットワークによって相互に通信可能な第 1 の通信装置と第 2 の通信装置との間で、トランスポート層以上の情報を利用した中継を行なうゲートウェイ装置において、

前記第 1 の通信装置と第 2 の通信装置との間で秘匿性を保証する通信のために、前記第 1 の通信装置と第 2 の通信装置との間に設定される第 1 のセキュリティアソシエーションに関する情報を保持する第 1 のセキュリティ情報保持手段と、

前記第 1 の通信装置と第 2 の通信装置との間で秘匿性を保証する通信を中継する際に前記第 1 のセキュリティアソシエーションに関する情報を利用して、前記第 2 の通信装置もしくは第 2 の通信装置に受信される暗号化された情報を復号化する情報復号化手段と、

前記復号化された情報に基づいて前記トランスポート層以上の情報を利用して中継処理を行う中継手段と、

前記中継手段が送信する情報を前記第 1 のセキュリティアソシエーションに関する情報を利用して秘匿化する情報暗号化手段と
を具備したことを特徴とするゲートウェイ装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、トランスポート層を利用する通信に介在する中継装置、通信装置、制御装置および通信制御方法に関する。

【0 0 0 2】

【従来の技術】

近年無線によって音声信号のみならず、データ通信も行なう要求が高まっている。TCP (Transmission Control Protocol) は、有線データ通信において信頼性のあるトランスポート層プロトコルとして広く使われているが、このプロトコルをそのまま無線に適用すると以下のような問題が発生する。

【0 0 0 3】

有線通信におけるTCPパケット損失はネットワークの輻輳を意味するため、TCPはパケット損失を検出するとデータの送出レートを下げて輻輳を回避するように設計されている。パケット損失は、同一シーケンス番号を持つACKが指定された数（通常はオリジナルに加えて3個）以上受信された場合、およびRTTとその偏差から定められるタイマがタイムアウトした場合に検出される。

【0004】

このため無線区間のエラーおよびハンドオフによるTCPパケット損失、乃至はリンク層でのエラー回復に時間がかかった場合も輻輳と解釈されるので、必要以上に輻輳回避を行う結果、スループットが利用できる無線帯域以下に低下する場合が多くなる。また、無線区間のエラーをエンド・エンドでTCPによって再送すると、有線部分の帯域が無駄であるし時間もかかる。また、リンク層がエラー回復をしている場合は同じデータを重複して送ることになる。

【0005】

このような問題を解決するために、有線側端末と無線側端末の間に（多くの場合は無線と有線の境界部分に）、TCPの性能を向上させるためのプロキシ（PEP：Performance Enhancement Proxy）を挿入する方法が提案されている。

【0006】

Split Connectionによる方法は、TCPコネクションをProxy（以下ではTCP-GWと呼ぶ）に於いて、有線側TCPコネクションと無線側TCPコネクションとに分割する方法である。有線端末から無線端末にデータを送信する場合を想定する。

【0007】

TCP-GWは無線端末の代わりに有線端末にACKを返すので、無線のエラーの影響（パケット損失乃至大きな遅延変動）は、有線端末から隠蔽される。TCPデータパケットが失われた場合には、TCP-GWが有線端末の代わりにデータの再送を行う。無線側のTCPは無線用にチューニングしたものであっても良い。例えば、無線側TCPはselective ACKオプション（IETF RFC2018）を使って、高いパケット損失率でも性能が大きく劣化しないようにしたものでも良い。また、輻輳制御のアルゴリズムを変更して、TCPパケット損失があっても、帯域を絞り過ぎない用にしたものでもよい。

【0008】

Snoop proxyによる方法は、TCP-GWがTCPコネクションを終端とみなしてしまうので、TCPのエンド・エンドセマンティクス（TCPのACKが送信端末に戻って来た場合には、そのACKのシーケンス番号までは受信端末に到達している）を破るという問題に対応するものである。Snoop proxyは、TCPデータパケットをバッファするが、その時点では送信端末にACKは返さない。本来の受信端末からのACKが帰って来た時点でACKを送信端末に中継し、バッファしていたTCPデータパケットを廃棄する。但し、ACKが重複ACKであり、本来の送信端末からの再送をトリガするものである場合、重複ACKは廃棄して、Snoop proxyがTCPデータパケットの再送を行う。また、Snoop proxyはタイムアウト再送も行う。このようにして、無線エラーの影響の大部分を、送信端末から隠蔽する。

【0009】

一方で、このような無線データ通信は、近隣の誰もが無線信号を傍受可能であり、かつ移動環境で使用する機会が多いため、セキュリティに対する要求も高くなる。

【0010】

インターネットにおけるセキュリティ確保の一方法として、IPSecによるものがある（IETF RFC2401, 2402, および2408など）。セキュリティは様々なレイヤで提供されるが、IPSecはIP層でセキュリティを確保するための方式である。IPSecでは、（1）IPヘッダの経路上で変更されない部分と、（2）IPペイロードに対してデータが経路上で改竄されていないことと、（3）そのデータが本来の送信者によって生成されたこと、を保証する機能がある。このためには、AH（Authentication Header）を、IPヘッダとIPペイロードとの間に挿入しなければならない。また、IPペイロードに対して、秘匿性、改竄のないこと、および送信者による生成を保証する機能もある。このためには、ESP（Encapsulating Security Payload）を用いる。なお、AHとESPを組み合わせることもできる。

【0011】

また、IPSecやMobileIPでは、IPSecやMobileIPの機能を持つゲートウェイ装置やエージェント装置で、本来のパケットを別のパケットに包んで（カプセル化）

して、ゲートウェイ装置やエージェント装置、乃至は本来のパケットの目的地である端末まで送信する技術が利用される。本来のパケットがカプセル化された状態で辿る経路をトンネルと表現する。

【 0 0 1 2 】

【発明が解決しようとする課題】

以上説明したように、無線網に收容された無線端末装置と有線網に收容された有線端末装置との間で通信を行う際に、TCP-GW乃至Snoop proxyのようなTCPの性能を向上させるための装置とIPSecのようなセキュリティを提供する方法とは、共に無線データ通信環境での要求が高いが、このような装置と方法とを組み合わせ使用する場合には以下に説明するような問題があった。

【 0 0 1 3 】

つまり、TCPヘッダはIPSecによって保護されているIPペイロードに含まれるが、TCPの性能を向上させるProxyは、TCPヘッダに含まれる情報を知り、かつ場合によって変更しなければならないことが問題である。また、送信されるデータに改竄のないことを保証すると、TCP-GWが本来の受信端末に代わってACKを送信することはできなくなる。これはTCP-GW自身がACK情報を生成する必要が生じてくるためである。更に送信されるデータに秘匿性を要求すると、TCP-GW乃至Snoop ProxyはTCPヘッダの情報が読み取れないので、有効な動作が不可能になる。

【 0 0 1 4 】

また、IPSecやMobileIPなどで利用される「トンネル」の途中にProxy装置がある場合、このproxy装置は有効に機能しない。なぜなら、例えばTCP-GWがカプセル化されたパケットを処理するべきか否かのフィルタにかけるために、カプセル化しているパケットのヘッダを調べても、そのヘッダはペイロードがTCPパケット

であることを表示していないからである。

【 0 0 1 5 】

そこで、本発明は上記従来の問題点に鑑みてなされたもので、TCP-GWやSnoopに代表されるProxy装置と、IPSecに代表されるセキュリティプロトコルとを組み合わせることによって、セキュリティを維持しつつ無線端末装置と有線端末装置

とのデータ通信を効率よく行い、またIPSecやMobileIPなどで利用される「トンネル」を通るカプセル化されたパケットに対しても有効に機能するゲートウェイ装置、通信装置、制御装置、および通信制御方法の提供を目的とする。

【 0 0 1 6 】

【課題を解決するための手段】

以上に述べた課題を解決するため、本発明におけるゲートウェイ装置は、無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継を行うゲートウェイ装置において、前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために、前記無線端末装置と前記有線端末装置との間に設定される第1のセキュリティアソシエーションに関する情報を保持する第1のセキュリティ情報保持手段と、前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信を中継する際に前記第1セキュリティアソシエーションに関する情報を利用して前記無線端末装置もしくは前記有線端末装置に受信される暗号化された情報を復号化する情報復号化手段と、前記復号化された情報に基づいて前記トランスポート層以上の情報を利用して中継処理を行う中継手段と、前記中継手段が送信する情報を前記第1のセキュリティアソシエーションに関する情報を利用して秘匿化する情報暗号化手段とから構成される。

【 0 0 1 7 】

また、本発明におけるゲートウェイ装置は、無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継を行うゲートウェイ装置において、前記無線端末装置と前記有線端末装置との間で情報の認証を保証した通信を行うために、前記無線端末装置と前記有線端末装置との間に設定される第1のセキュリティアソシエーションに関する情報を保持する第1のセキュリティ情報保持手段と、前記無線端末装置と前記有線端末装置との間で前記認証を保証された情報を前記トランスポート層以上の情報を利用して中継処理を行う中継手段と、前記中継手段が中継する前記認証が保証された情報および前記中継手段が必要に応じて新たに生成した情報に対して前記第1のセキュリティアソシエーションに関する情報を利用して、前記認証が保証された情

報を保証する認証情報を付加する認証情報手段とから構成される。

【 0 0 1 8 】

また、本発明の通信装置は、無線網に收容された無線端末装置もしくは有線網に收容された有線端末装置のいずれかに設けられ、前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第1のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第2のセキュリティアソシエーションに関する情報を、前記無線端末装置と前記有線端末装置との間でトランスポート層以上の情報を用いた中継を行うゲートウェイ装置に提供するセキュリティ情報提供手段とから構成される。

【 0 0 1 9 】

また、本発明における制御装置は、無線網に收容された無線端末装置と有線網に收容された有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第1のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第2のセキュリティアソシエーションに関する情報を生成するセキュリティ情報生成手段と、前記生成された第1乃至第2のセキュリティアソシエーションを前記無線端末装置乃至前記有線端末装置に配布するセキュリティ情報配布手段とから構成される。

【 0 0 2 0 】

また、本発明の制御装置は、無線網に收容された無線端末装置と有線網に收容された有線端末装置との間でトランスポート層以上の情報の中継の制御を行う制御装置において、前記無線端末装置と前記有線端末装置に設けられた検索鍵に対する、前記無線端末装置乃至前記有線端末装置に設けられた検索鍵に対して、前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第1のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前

記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第2のセキュリティアソシエーションに関する情報を検索し抽出するセキュリティ情報検索手段とから構成される。

【0021】

また、本発明における通信装置は、無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継を行う通信装置において、前記情報の内容に基づいて前記無線端末装置と前記有線端末装置との間で中継処理を行う中継手段を動作させるか否かを選択し、前記中継手段を動作させる場合には前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第1のセキュリティアソシエーションに関する情報、乃至前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第2のセキュリティアソシエーションに関する情報を用いて通信を行い、前記中継手段を動作させない場合には前記無線端末装置と前記有線端末装置との間で通信を行うための第3のセキュリティアソシエーションに関する情報を設定し通信を行わせる選択手段とから構成される。

【0022】

また、本発明の通信制御方法は、無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でゲートウェイ装置を介してトランスポート層以上の情報の中継を行う通信制御方法において、第1のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第1のセキュリティアソシエーションに関する情報、乃至前記第1のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第2のセキュリティアソシエーションに関する情報を、第2のゲートウェイ装置に引き渡す工程と、前記無線端末装置と前記有線端末装置との間の前記秘匿性乃至前記認証を保証した通信が、前記第1のゲートウェイ装置から前記第2のゲートウェイ装置に変化

して経由された場合に、前記第 1 のゲートウェイ装置で行っていた前記トランスポート層以上の情報を利用した中継処理を前記引き渡された第 1 及び第 2 のセキュリティアソシエーションに関する情報を利用して前記第 2 のゲートウェイ装置において動作される工程とを有する。

【 0 0 2 3 】

また、本発明における通信制御方法は、無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でゲートウェイ装置を介してトランスポート層以上の情報の中継を行う通信制御方法において、第 1 のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で秘匿性を保証する通信のために前記無線端末装置と前記有線端末装置との間に設定される第 1 のセキュリティアソシエーションに関する情報、乃至前記第 1 のゲートウェイ装置を介して前記無線端末装置と前記有線端末装置との間で前記情報の認証を保証した通信を行うために前記無線端末装置と前記有線端末装置との間に設定される第 2 のセキュリティアソシエーションに関する情報を、第 2 のゲートウェイ装置に引き渡す工程と、前記無線端末装置と前記有線端末装置との間の前記秘匿性乃至前記認証を保証した通信が、前記第 1 のゲートウェイ装置から前記第 2 のゲートウェイ装置に変化して経由された場合に、前記第 1 のゲートウェイ装置で行っていた前記トランスポート層以上の情報を利用した中継処理を前記引き渡された第 1 及び第 2 のセキュリティアソシエーションに関する情報及び前記トランスポート層以上の状態を利用して前記第 2 のゲートウェイ装置において動作される工程とを有する。

【 0 0 2 4 】

また、本発明におけるゲートウェイ装置は、無線網に収容された無線端末装置と有線網に収容された有線端末装置との間でトランスポート層以上の情報の中継を行うゲートウェイ装置において、第 1 のゲートウェイ装置を通過した前記情報をカプセル化する第 2 のゲートウェイ装置と、前記カプセル化された情報からカプセルを取り除き、前記カプセルが取り除かれた情報を前記トランスポート層以上の情報を利用して中継を行う必要があるか否かを判断し、必要な場合には中継を行う第 3 のゲートウェイ装置と、前記第 3 のゲートウェイ装置から送られた情

報をカプセル化するカプセル化手段とから構成される。

【 0 0 2 5 】

また、本発明におけるゲートウェイ装置は、ネットワークによって相互に通信可能な第 1 の通信装置と第 2 の通信装置との間で、トランスポート層以上の情報を利用した中継を行なうゲートウェイ装置において、前記第 1 の通信装置と第 2 の通信装置との間で秘匿性を保証する通信のために、前記第 1 の通信装置と第 2 の通信装置との間に設定される第 1 のセキュリティアソシエーションに関する情報を保持する第 1 のセキュリティ情報保持手段と、前記第 1 の通信装置と第 2 の通信装置との間で秘匿性を保証する通信を中継する際に前記第 1 のセキュリティアソシエーションに関する情報を利用して、前記第 2 の通信装置もしくは第 2 の通信装置に受信される暗号化された情報を復号化する情報復号化手段と、前記復号化された情報に基づいて前記トランスポート層以上の情報を利用して中継処理を行う中継手段と、前記中継手段が送信する情報を前記第 1 のセキュリティアソシエーションに関する情報を利用して秘匿化（暗号化）する情報暗号化手段とから構成される。

【 0 0 2 6 】

また、本発明におけるゲートウェイ装置は、ネットワークによって相互に通信可能な第 1 の通信装置と第 2 の通信装置との間で、トランスポート層以上の情報を利用した中継を行なうゲートウェイ装置において、前記第 1 の通信装置と第 2 の通信装置との間で秘匿性を保証する通信のために、前記第 1 の通信装置と第 2 の通信装置との間に設定される第 1 のセキュリティアソシエーションに関する情報を保持する第 1 のセキュリティ情報保持手段と、前記第 1 の通信装置と第 2 の通信装置との間で秘匿性を保証する通信を中継する際に前記第 1 のセキュリティアソシエーションに関する情報を利用して、前記第 2 の通信装置もしくは第 2 の通信装置に受信される暗号化された情報を復号化する情報復号化手段と、前記復号化された情報に基づいて前記トランスポート層以上の情報を利用して中継処理を行う中継手段と、前記中継手段が送信する情報を前記第 1 のセキュリティアソシエーションに関する情報を利用して秘匿化する情報暗号化手段とから構成される。

【 0 0 2 7 】

なお、無線通信端末および有線通信端末は、それら装置と情報の送受信もしくは中継がなされるサーバを含んだものであっても良い。また、通信装置は無線通信端末、有線通信端末乃至ルータであっても良い。

【 0 0 2 8 】

【発明の実施の形態】

以下、本発明の実施の形態について図面を参照して説明する。

【 0 0 2 9 】

図 1 は本発明のネットワーク構成図であり、ルータ 7 0 1 を挟んで、ネットワーク 2 0 1 側とネットワーク 2 0 2 側とに分けられる。これらの間でネットワーク運営の主体が異なっても構わない。ネットワーク 2 0 1 は有線網に有用された TCP/IP 端末 1 0 1 ~ 1 0 3 (有線端末装置) を収容し、IP パケットを交換するルータ 7 0 1 によってネットワーク 2 0 2 と相互接続されている。ここで、ネットワーク 2 0 1 と類似のネットワークが複数ネットワーク 2 0 2 に接続されていても良い。また、ネットワーク 2 0 1 がネットワーク 2 0 2 以外のネットワークと相互接続されていても良い。ネットワーク 2 0 2 側は移動をサポートしているものとする。但し、移動の有無は特許の本質とは無関係である。移動は Mobile IP のような IP 層による実現、セルラー網のようなリンク層による実現などがあるが、その方法も問わない。移動を実現するために必要な要素は図示していない。ネットワーク 2 0 2 は TCP-GW 4 0 1 と 4 0 2 とによってネットワーク 2 0 3 と 2 0 4 とを、TCP-GW 4 0 3 によって基地局 3 0 5 と 3 0 6 とを、それぞれ収容する。

【 0 0 3 0 】

TCP-GW は Snoop Proxy のような TCP を意識したリンク層再送機能を持つノードであっても良いし、更に一般的なプロキシ装置であっても構わないが、以下では TCP-GW で代表する。更にネットワーク 2 0 2 はセキュリティサーバ 6 0 1 を持つ。ネットワーク 2 0 3 と 2 0 4 は、それぞれ基地局 3 0 1 と 3 0 2、基地局 3 0 3 と 3 0 4 を収容する。基地局 3 0 1 のエリアには無線網に収容された移動端末 5 0 1 と 5 0 2、基地局 3 0 2 のエリアには無線網に収容された移動端末 5 0 3

、基地局304のエリアには無線網に収容された移動端末504と505、基地局305のエリアには無線網に収容された移動端末506、そして基地局306のエリアには無線網に収容された移動端末507と508が存在する状態を示している。移動端末501～508（無線端末装置）はTCP/IP端末である。

【0031】

このような状況下で、例えば端末101と移動端末501の間でIPSecを利用してセキュリティを保証したTCP/IP通信を行う場合を想定する。IPSecによる通信を行うためには、端末101と移動端末501との間にIPSec SA (Security Association、以下SAと記す) が確立されている必要がある。

【0032】

SAは一方向の関係を示すので、双方向の関係には2つのSAが必要となる。1つのSAに適用されるセキュリティプロトコルは1つに制限される。但し、必要なら2点の間で複数のSAを設定しても良い。SAを識別する情報は、(1) SPI (Security Parameter Index)、(2) IP destination address、(3) Security protocol identifierの3つである。SPIはローカルで一意的なビット列である。SPIは、AHおよびESPヘッダに含まれ、受信側が受信パケットを処理するために必要なSAを決定するために使われる。IP destination addressはSAの終点を示す。SAの終点はエンドユーザシステムであっても、ファイアウォールのようなものであっても良い。Security protocol identifierは、SAがAH乃至ESPを使うか否かを示す。

【0033】

セキュリティアソシエーションデータベース (SAD) には、以下のような情報が含まれる。

【0034】

- ・シーケンス番号カウンタ：AH乃至ESPヘッダのシーケンス番号フィールドを生成するために使用される。

【0035】

- ・シーケンス番号カウンタオーバフロー：オーバフローした場合は、それ以上のパケット送信は禁止される。

【 0 0 3 6 】

・ Anti-reply ウィンドウ: AHまたはESPパケットが第3者による再送でないことを保証するために、そのシーケンス番号は、ここで指定されるスライディングウィンドウの範囲になければならない。

【 0 0 3 7 】

・ AH情報: 認証アルゴリズム、鍵、鍵の生存時間、およびAHに関連するパラメータ。

【 0 0 3 8 】

・ ESP情報: 暗号化と認証アルゴリズム、鍵、初期化の値、鍵の生存時間、およびESPに関連するパラメータ。

【 0 0 3 9 】

・ SAの生存時間: このSAが新たなSAで置き換えられなければならない、時間インターバル、乃至はバイト数。およびこのような置き換えを行わなければならないか否かの指定。

【 0 0 4 0 】

・ IPSecプロトコルモード: トンネル、トランスポート乃至ワイルドカードモード。

【 0 0 4 1 】

・ Path MTU: 観測されたパスの最大transmission unit (IPフラグメントなしでそのパス経由で伝送できる最大サイズ)。およびその情報の新しさ。

【 0 0 4 2 】

ユーザのポリシーによって、IPSecをいかにIPトラフィックに適用するかを決めることができる。つまりIPSecを適用するか否か、適用するとすればどのSAを利用するかを選択できる。このような情報はセキュリティポリシーデータベース (SPD) に含まれている。

【 0 0 4 3 】

SPDのエントリは、以下のselectorによって定められる。

【 0 0 4 4 】

・ Destination IP address: 範囲を示すものであっても良い。

【 0 0 4 5 】

- ・ Source IP address: 範囲を示すものであっても良い。

【 0 0 4 6 】

- ・ User ID: システムのユーザ識別子。

【 0 0 4 7 】

- ・ Data sensitivity level: 秘密乃至そうでないかなど。

【 0 0 4 8 】

- ・ トランスポート層プロトコル: UDP, TCPなどを指定するプロトコル番号。

【 0 0 4 9 】

- ・ IPsec プロトコル: AH, ESP乃至AH/ESP。

【 0 0 5 0 】

- ・ Source and destination ports: TCP乃至UDPのポート番号。

【 0 0 5 1 】

- ・ IPv6 class, IPv6 flow label
- ・ IPv4 Type of Service (TOS)

このように識別されるSPDの各エントリには、1つ以上のSAが対応している。

【 0 0 5 2 】

SAは手動で設定しても良いが、Internet Key Exchange (IKE) によって自動的に設定することも可能である。IKEは2つのフェーズに分けられる。フェーズ1では、IKE SAを確立しその後の通信の安全を図る。フェーズ2では、IKE SAの下で、AH乃至はESPのためのSAのパラメータを交換する。

【 0 0 5 3 】

さて、TCP-GWに代表されるプロキシが機能するためには、TCP-GWがSAの少なくとも一部の情報を知っている必要がある。この情報とはより具体的には、暗号化を解いて必要な処理後に再び暗号を掛けるために必要な情報であり、また、プロキシがパケットを生成する場合にそのパケットを正しく認証された形式にするために必要な情報である。

【 0 0 5 4 】

このようなプロキシを機能させるための方法として、以下の方式が考えられ

る。

【 0 0 5 5 】

(方式 1) 各種情報を手動で設定する。

【 0 0 5 6 】

(方式 2) IKE のフェーズ 2 で交換される SA 情報から得る。つまり、IKE SA の情報を知っていて IPsec SA 情報を傍受したエンティティがプロキシに情報を与える。

【 0 0 5 7 】

(方式 3) SA のいずれかの端点から提供を受ける。

【 0 0 5 8 】

(方式 4) プロキシ自ら、乃至セキュリティサーバが SA 情報を生成し、各端点と必要ならプロキシに提供する。

【 0 0 5 9 】

以下では、方式 3 と方式 4 について詳しく述べる。

【 0 0 6 0 】

最初に (方式 3) について述べる。端末 1 0 1 と移動端末 5 0 1 の間で、IKE SA が確立されているとする。これから行おうとする通信に適用すべき IPsec SA は、確立されている場合と確立されていない場合とがある。IPsec SA 確立されていない場合は、端末 1 0 1 のセキュリティ情報管理 1 1 2 4 (図 3 参照、セキュリティ情報提供手段 (請求項 3)) と移動端末 5 0 1 のセキュリティ情報管理 1 5 2 4 (図 4 参照、セキュリティ情報提供手段 (請求項 3)) の間で、IKE のフェーズ 2 の手順で IPsec SA を確立すれば良い。セキュリティ情報管理 1 1 2 4 (選択手段 (請求項 7))、1 5 2 4 は、自らの持つ SAD と SPD に、この IPsec SA 確立で発生した関連する情報を記憶する。なお、IPsec SA として、プロキシの介在を許容するものと、許容しないものを設けても良い。更に、プロキシに暗号を解くことは許すが、新たなパケットの生成乃至パケット内容の変更は許容しないクラスがあっても良い。これは SPD の selector の data sensitivity level に、その識別を行う分類を設けるのが自然であるが、例えばポート番号で識別しても良い。

【 0 0 6 1 】

以下では、プロキシの介在を許容するIPSec SAを主に扱う。プロキシの介在を許容しないIPSec SAについては、従来のIPSecと同様に動作する。

【 0 0 6 2 】

さて、端末101と移動端末501は、セキュリティサーバ601（セキュリティ情報生成手段（請求項5）、セキュリティ情報配布手段（請求項5）、制御装置（請求項6））およびTCP-GW401～403を信頼できる装置として扱う。例えば、それらがある信頼できるネットワーク運営主体によって信頼できる装置として運用されている場合が想定できる。このネットワークのTCP-GWに代表されるプロキシ機能を利用するためには、セキュリティサーバ601にIPSec SA情報を提供する必要がありますことは、端末101乃至移動端末501の少なくともいずれか一方には認識されていることを仮定している。なお、セキュリティサーバ601でなく、TCP-GW401に直接IPSec SA情報を提供してもTCP-GWとして有効に動作できるが、利用する個別のプロキシを端末101乃至移動端末501が認識しなければならない。TCP-GWやSnoopなどは、本来その存在が端末から見えないので、これはあまり良い方法ではない。また、端末101、移動端末501のいずれが提供しても良いが、無線対応のプロキシを利用すべきであることをより容易に把握できる移動端末501が提供すると仮定する。まず、これから送信するIPSec SA情報を保護するために、移動端末501とセキュリティサーバ601の間に何らかのセキュリティアソシエーションが必要である。セキュリティアソシエーションは、IPSecを使うと仮定する。移動端末501とセキュリティサーバ601の間で、最初にIKE SAを確立し、次にAHとESPの両方を用いるIPSec SAを確立する。このIPSec SAを用いて、移動端末501のセキュリティ情報管理1524から、セキュリティサーバ601のセキュリティ情報管理1624（図5参照、セキュリティ情報生成手段（請求項5）、セキュリティ情報配布手段（請求項5）、セキュリティ情報検索手段（請求項6））に向けて、端末101と移動端末501の間のプロキシ介在を許容するIPSec SA情報を送信する。セキュリティ情報管理1624は、この情報をSPDとSADに記憶する。

【 0 0 6 3 】

図2はTCP-GWのブロック構成図であり、上述したSnoop Proxyのようなものであっても良くその場合の構成は異なる。また図3は端末101のブロック構成図であり、図4は移動端末501のブロック構成図であり、図5はセキュリティサーバ601のブロック構成図である。なお、図中の実線矢印はデータの流れ、破線矢印は制御の流れを示す。

【0064】

以下で、TCP-GW401は、端末101と移動端末501の間のトラフィックを検出したことを契機に、IPSec SA情報をセキュリティサーバ601から取得する。ここでは、IKE SAによって、上記のプロキシ介在を許容するIPSec SAを確立するためのトラフィックを検出したとする。IKEはUDPのポート番号500を利用しているので、IP入力部1423でIPヘッダを見ていれば、この通信の存在がわかる。端末101と移動端末501の間の他の種類の通信であっても構わない。これらの存在は、端末101と移動端末501の間で、今後も何らかの通信が行われる可能性が高いことを示している。従って、TCP-GW401のセキュリティ情報管理1424（第1のセキュリティ情報保持手段（請求項1，2））が、セキュリティサーバ601のセキュリティ情報管理1624に対して、端末101と移動端末501の間のIPSec SAに関する情報を提供するように要求する。例えば端末101と移動端末501のIPアドレスの組を検索鍵として予めセキュリティサーバ601に記憶しておくことも一手法である。

【0065】

セキュリティサーバ601のセキュリティ情報管理1624は、TCP-GW401のセキュリティ情報管理1424からの要求を受けた時点では、まだ端末101と移動端末501の間のIPSec SAを持っていないかも知れない。なぜなら、この要求はIPSec SAを設定するためのトラフィックを検出して行われたものだからである。セキュリティ情報管理1624は、そのような要求があったことをタイムアウトするまで記憶しておいて、要求にあうIPSec SA情報を得る度に、TCP-GW401のセキュリティ情報管理1424に、IPSec SA情報を提供する。

【0066】

このようにして、TCP-GW401のセキュリティ情報管理1424が、セキュリ

ティサーバ 6 0 1 のセキュリティ情報管理 1 6 2 4 から、端末 1 0 1 と移動端末 5 0 1 の間のIPSec SAに関する情報を得ると、これをセキュリティ情報管理 1 4 2 4 のSPDとSADに記憶する。更に、IP入力部 1 4 2 3 でフィルタを設定して、端末 1 0 1 と移動端末 5 0 1 の間のプロキシ介入を許容するIPSec SAによるパケットでかつTCPの通信であるという条件にマッチする時には、TCP層まで上げるようにする。なお、IPSec SA情報要求がタイムアウトする時点で、更に端末 1 0 1 と移動端末 5 0 1 の間での通信がTCP-GW 4 0 1 を通過すると見込まれる場合には、要求を更新する。

【 0 0 6 7 】

次に、プロキシ介入を許容するIPSec SAを利用して、端末 1 0 1 のPEP利用アプリケーション 1 1 6 2 (図 3 参照) と移動端末 5 0 1 のPEP利用アプリケーション 1 5 6 2 (図 4 参照) が通信を行う。なお、アプリケーションでプロキシ介入を許容するか否かを分けているのは便宜的なもので、実際にはTCPのコネクション毎に使い分けが可能である。PEP利用アプリケーション 1 1 6 2 がPEP利用アプリケーション 1 5 6 2 に対して、TCPのコネクション設定を行うとする。PEP利用アプリケーション 1 1 6 2 は、例えばUNIXのsocketインタフェースによって、OSに対してTCPコネクション設定を要求できる。この際、例えばsocketのオプションによって、このTCPコネクションをプロキシ介入を許容するか否かを指定できる。既に述べたように、ここではプロキシ介入を許容する。これは、例えばSPDエントリのData sensitivity level selectorの値として設定される。他のselectorの値は、destination IP addressとして移動端末 5 0 1 のIPアドレス、source IP addressとして端末 1 0 1 のIPアドレス、UserIDとしてPEP利用アプリケーション 1 1 6 2 のユーザ識別子、Transport layer protocolとしてTCP、IPSec protocolとして例えばAH/ESP (他にAHあるいはESPが可能)、source/destination portとして適当なポート番号などとなる。IP出力部 1 1 2 2 を監視しているセキュリティ情報管理 1 1 2 4 は、出力IPパケット毎にSDPエントリを検索し、対応するIPSec SAを見付ける。Selectorが上記の値を持つパケットに対しては、既に述べたプロキシ介入を許容するIPSec SAが対応する。するとセキュリティ情報管理 1 1 2 4 は、IPSec SAに指定されたアルゴリズムと鍵などによって、パケ

ットを暗号化し認証のための情報を付加するように、暗号機能 1 1 2 6 と認証機能 1 1 2 5 を制御する。トランスポートモードとトンネルモードのうち、ここでは前者を利用するので、図 6 (a) のパケットを処理後のパケットは図 6 (b) に示すフォーマットになる。ここで、一般に暗号化後には TCP ヘッダとデータの境界は保存されない。また、AH 認証対象は、IP ヘッダの経路上での変化による結果を予測できない部分（例えば TTL など）は含まない。

【 0 0 6 8 】

このように処理されたパケットは、有線 IF 出力部 1 1 4 2 によってネットワーク 2 0 1 に送信され、更にルータ 7 0 1、ネットワーク 2 0 2 を経由して、TCP-GW 4 0 1 に到着する。有線側 IF 入力部 1 4 4 6 を経て IP 入力部 1 4 2 3 に到着したパケットは、SPI (Security Parameter Index)、IP destination address、Security protocol identifier の 3 つによって識別される IPsec SA の指定に従って処理される。識別するパラメータの値は、セキュリティサーバ 6 0 1 から提供されたものであり、セキュリティ情報管理 1 4 2 4 によって IP 入力部に設定されている。セキュリティ情報管理 1 4 2 4 が認証機能 1 4 2 5 (認証情報手段 (請求項 2)) と暗号機能 1 4 2 6 (情報復号化手段 (請求項 1)、情報暗号化手段 (請求項 1)) を制御して、図 6 (b) に示す IPsec パケットを、図 6 (a) に示す元のパケットの形に戻す。

【 0 0 6 9 】

元のパケットの情報から TCP 中継処理を行うか否かを IP 入力部 1 4 2 3 が判断し、中継処理を行うものとして TCP 入力部 1 4 0 5 に渡す。最も単純な判断基準は TCP なら全て TCP 接続を利用して中継するというものであるが、他の属性も使用して TCP だが TCP 情報を利用した中継をしないようにしても良い (IP 中継となる)。このパケットは、その内容に応じて、TCP 中継部 1 4 0 2 (中継手段 (請求項 1, 2)) の有線→無線 1 4 0 7、TCP 入力部 1 4 0 5 および無線 TCP 出力部 1 4 0 8 で処理される。例えば、SYN パケットなら、新たな TCP コネクションが設定されるものとして対応する状態を生成する。必要なら適当なオプションを追加するなどして、無線 TCP 出力部 1 4 0 8 に中継する。更に、TCP 出力部 1 4 0 4 から SYN/ACK を返す (Snoop の場合は返さない)。別の例として、データパケットなら、

後で再送する可能性があるので、バッファにコピーを蓄積してから、無線TCP出力部 1 4 0 8 に渡す。更に、TCP出力部 1 4 0 4 からそのデータパケットに対するACKを返す（Snoopの場合は返さない）。なお、ここで扱っているパケットは、TCP-GW 4 0 1 が生成したものを含め、全て端末 1 0 1 と移動端末 5 0 1 の間で送受信されているかのように、IPヘッダのアドレスフィールドが設定されている。つまり、TCPゲート 4 0 1 存在は隠されている。

【 0 0 7 0 】

無線TCP出力部 1 4 0 8 およびTCP出力部 1 4 0 4 は、パケットをIP出力部 1 4 2 2 に渡す。セキュリティ情報管理 1 4 2 4 は、パケットの情報からSPDのエントリを識別するselector情報を得て、SPDを検索して対応するIPSec SAを得る。このIPSec SAに関する情報をSADから取得して、それに応じて暗号機能 1 4 2 6 と認証機能 1 4 2 5 を制御して、再びパケットを図 6（b）に示すIPSecパケットの形にする。ここで同じパケットであっても、TCP-GWに受信されたIPSecパケットと、TCP-GWから送信されるIPSecパケットの内容は一般に異なる。例えば、TCP-GW 4 0 1 は、ACKを中継するのではなく生成するので訂正のために付与されるIPSecのAHないしESPのシーケンス番号は一般に異なる。これらのパケットは、無線側IF出力部 1 4 4 3 からネットワーク 2 0 3 へ、有線側IF出力部 1 4 4 5 からネットワーク 2 0 2 へ、それぞれ送信される。

【 0 0 7 1 】

なお、Snoopの場合は、Snoop proxyに受信されたIPSecパケットと、Snoop proxyから送信されるIPSecパケットの内容は多くの場合同じにできる。

【 0 0 7 2 】

Snoopは重複ACKを中継せずに捨てることがあるが、これはIPネットワーク内で自然に失われるのと同じであり、IPSec的に特に問題無い。Snoopが本来のTCP送信ホストの代わりに再送を行うことがあるが、これはオリジナルのコピーを再送すれば良いが、IPSecのAnti-replyによって受信端末で捨てられる可能性がある。これを防ぐためには、認証のためのシーケンス番号が、Anti-replyウィンドウの範囲内に収まっている必要がある。これらの条件が満たされれば、Snoopの場合には、IPSecパケットから元のTCP/IPヘッダ情報を取り出せば良いのであ

て、一度オリジナルの形に戻したパケットを再びIPSecパケットに変更する必要は無い。従って、Snoop proxyに認証を掛けるために鍵情報を与えなければ、端末101と移動端末501の間で、情報の改竄がなかったことと、本来の送信者から送信されたパケットであることはIPSec的に保証できる。Snoop proxyに暗号を解くためのSA情報を持てば機能できる。

【0073】

ネットワーク203へ送信されたパケットに注目すると、これは基地局301経由で移動端末501によって受信される。無線IF入力部1543を経てIP入力部1523に到着したパケットは、SPI (Security Parameter Index)、IP destination address、Security protocol identifierの3つによって識別されるIPSec SAの指定に従って処理される。セキュリティ情報管理1524が認証機能1525と暗号機能1526を制御して、図6(b)に示すIPSecパケットを、図6(a)に示す元のパケットの形に戻す。そして、パケットに載っていた情報は、PEP利用アプリケーション1562に渡される。

【0074】

次に(方式4)、つまりセキュリティサーバ601がIPSec SA情報を生成し、端末101と移動端末501、およびTCP-GW401に生成したIPSec SA情報を渡す場合について述べる。

【0075】

移動端末501のセキュリティ情報管理1124が、セキュリティサーバ601のセキュリティ情報管理1624に対し、端末101との間のプロキシの介在を許容するIPSec SA情報を生成するように依頼する。依頼にはIPSecなどでセキュリティの確保された通信路を用いる。セキュリティ情報管理1624は、依頼に応じたIPSec SA情報を生成すると、これをセキュリティの確保された通信路で、移動端末501、端末101、およびTCP-GW401に提供する。移動端末501には、依頼の応答として提供すれば良い。端末101に対しては、セキュリティサーバ601から直接提供しても良いし、移動端末501から提供しても良い。TCP-GWに対しては、例えば移動端末501の位置情報から、TCP-GW401がIPSec SAを利用する可能性の高いと判断できれば、セキュリティサーバ601が

自発的に送信すれば良い。さもなければTCP-GW 4 0 1 が、端末 1 0 1 と移動端末 5 0 1 の間の通信を検出してから、セキュリティサーバ 6 0 1 に要求することになる。全てのTCP-GW 4 0 1 ～ 4 0 3 に提供しても機能するが、効率は悪いし、セキュリティが破られる可能性も高くなる。これらの通信は、端末 1 0 1、移動端末 5 0 1、TCP-GW 4 0 1、およびセキュリティサーバ 6 0 1 それぞれのセキュリティ情報管理 1 1 2 4、1 5 2 4、1 4 2 4、および 1 6 2 4 の間で行われる。一旦、IPSec SA の情報がTCP-GW 4 0 1 に提供されれば、後の動作は（方式 3）の場合と同様であるので省略する。

【 0 0 7 6 】

これから、移動端末（例えば移動端末 5 0 1）の移動に伴いTCP-GWを変更するプロキシ-ハンドオフ制御について述べる。このため、移動端末 5 0 1 で終端される中継対象のTCPコネクション状態の情報と、移動端末 5 0 1 に対応するIPSec SA情報を、前のTCP-GW（例えばTCP-GW 4 0 1）から後のTCP-GW（例えばTCP-GW 4 0 2）に引き継ぐ必要がある。TCP-GW 4 0 2 は、移動端末 5 0 1 を起点・終点とする通信を検出した際に、前のTCP-GWを何らかの方法で探して、ハンドオフ処理を行うために必要な情報を要求する。このために予め隣接するTCP-GWをお互いに認識しておくことが有効である。

【 0 0 7 7 】

例えば、

（NR方式A）物理的な距離が近いTCP-GWを認識する、

（NR方式B）ネットワーク的な距離（ホップ数、遅延など）が近いTCP-GWを認識する、

といった方式が考えられる。

【 0 0 7 8 】

移動端末の物理的な移動によりハンドオフが必要になるとすると、（NR方式A）が望ましい。しかし、物理的な位置を知ることができない場合には、（NR方式B）を利用する場合もある。

【 0 0 7 9 】

（NR方式A）を実現するために、例えばプロキシ管理サーバ 8 0 1 を設ける。

TCP-GW4 0 1 は基地局 3 0 1 と 3 0 2、TCP-GW4 0 2 は基地局 3 0 3 と 3 0 4、TCP-GW4 0 3 は基地局 3 0 5 と 3 0 6 の物理的な位置を何らかの方法で知りえており、その情報をプロキシ管理サーバ 8 0 1 に通知する。プロキシ管理サーバ 8 0 1 は、TCP-GW4 0 1 と 4 0 2 の間のハンドオフ、TCP-GW4 0 2 と 4 0 3 の間のハンドオフが発生し得ると判断する。そして、TCP-GW4 0 1 に対してはTCP-GW4 0 2 がハンドオフ対象となること、TCP-GW4 0 2 に対してはTCP-GW4 0 1 と 4 0 3 がハンドオフ対象となること、TCP-GW4 0 3 に対してはTCP-GW4 0 2 がハンドオフ対象となることを通知する。これらの処理は、TCP-GW4 0 1 ～ 4 0 3 のTCP ハンドオフ制御 1 4 1 0 とプロキシ管理サーバ 8 0 1 によって行われる。もちろん、TCP-GW4 0 1 ～ 4 0 3 に対して、これらの情報を手動で設定することも可能である。

【 0 0 8 0 】

また、(NR方式B) を実現するためには、例えば次のような手順が考えられる。

【 0 0 8 1 】

全てのTCP-GWが加入するマルチキャストグループを定義しておき、各TCP-GWのTCPハンドオフ制御 1 4 1 0 がTTLを適当に制限したマルチキャストパケットを問い合わせするために送信する。これを受信した各TCPハンドオフ制御 1 4 1 0 が送信元にユニキャストで応答することで、ホップ数の少ないTCP-GWを探すことができる。

【 0 0 8 2 】

さて、上述したように、端末 1 0 1 と移動端末 5 0 1 の間で、プロキシ介入を許容するIPSec SAの下で、TCP-GW4 0 1 を介して、TCPによる通信を行っているとす。プロキシハンドオフに伴う情報の引渡しにはいくつかのバリエーションが考えられる。

- ・ハンドオフする可能性のあるTCP-GWに、予め渡せる情報は渡しておくか否か。予め渡すとすれば以下のような候補がある。

【 0 0 8 3 】

- －中継対象端末：新しいTCP-GWがこの端末の通信を検出した時に、どのTCP-G

Wに問い合わせれば、必要な情報が得られるかがわかる。

【 0 0 8 4 】

ーIPSec SA情報:ハンドオフ遅延の減少が見込める。

・ユニキャストで問い合わせるか、マルチキャストで問い合わせるか。

【 0 0 8 5 】

ーユニキャスト:前のTCP-GWである可能性のある全てのTCP-GWに個別に問い合わせる。上記中継対象端末情報またはIPSec SA情報を持っていれば、その情報を提供したTCP-GWに問い合わせる。

【 0 0 8 6 】

ーマルチキャスト: 前のTCP-GWである可能性のある全てのTCP-GWを含むマルチキャストグループを定義しておく。このマルチキャストグループ宛に問い合わせを送信する。

【 0 0 8 7 】

なお、ハンドオフに伴う通信は、原則としてセキュリティが確保された通信路によって行う。

【 0 0 8 8 】

ここで、TCP-GW 4 0 1 のセキュリティ情報管理 1 4 2 4 から、TCP-GW 4 0 2 のセキュリティ情報管理 1 4 2 4 に対して、予めIPSec SA情報が与えられているとする。TCP-GW 4 0 1 のセキュリティ情報管理 1 4 2 4 は、セキュリティサーバ 6 0 1 から新たなIPSec SA情報を得ると、TCPハンドオフ制御 1 4 1 0 に、そのIPSec SA情報を提供すべき先のTCP-GWを問い合わせる。この場合はTCP-GW 4 0 2 に提供すべきなので、TCP-GW 4 0 1 のセキュリティ情報管理 1 4 2 4 は、TCP-GW 4 0 2 のセキュリティ情報管理 1 4 2 4 に対して、そのIPSec SA情報を提供する。TCP-GW 4 0 2 のセキュリティ情報管理 1 4 2 4 は、IPSec SA情報をSPDとSADに記憶すると共に、その提供元がTCP-GW 4 0 1 であることと、その提供時間を記憶する。

【 0 0 8 9 】

移動端末 5 0 1 が基地局 3 0 1 のエリアから、基地局 3 0 2 のエリアを経て、更に基地局 3 0 3 のエリアへ移動したとする。するとTCP-GW 4 0 2 が端末 1 0 1

と移動端末 5 0 1 の間の通信を検出する。TCP-GW 4 0 2 のセキュリティ情報管理 1 4 2 4 は、端末 1 0 1 と移動端末 5 0 1 の間の IPsec SA 情報を、最近提供したものが TCP-GW 4 0 1 であることを認識するので、TCP ハンドオフ制御 1 4 1 0 に対して、TCP 中継のハンドオフに必要な情報は、TCP-GW 4 0 1 から得られることを教える。また、TCP-GW 4 0 2 のセキュリティ情報管理 1 4 2 4 は、TCP-GW 4 0 3 のセキュリティ情報管理 1 4 2 4 に対して、対応する IPsec SA 情報を通知する。以前から知っていた IPsec SA 情報をこの時点で通知するのは、TCP-GW 4 0 3 へのハンドオフの可能性が生じたからである。

【 0 0 9 0 】

TCP-GW 4 0 2 の TCP ハンドオフ制御 1 4 1 0 は、TCP-GW 4 0 1 の TCP ハンドオフ制御 1 4 1 0 から得た、端末 1 0 1 と移動端末 5 0 1 間の TCP コネクションの情報から、TCP 1 4 0 1 と無線 TCP 1 4 0 3 に対して TCP 中継に必要な情報を設定する。例えば、シーケンス番号やウィンドウ制御関連の情報、設定されている TCP オプション、バッファに一時記憶されているデータパケットなどである。TCP 中継の再開にあたっては、TCP シーケンス番号がなるべく乱れ無いように行う。つまり、バッファに一時記憶されているデータパケットの TCP シーケンス番号が、端末 1 0 1 と移動端末 5 0 1 の間を流れている TCP データパケットのシーケンス番号よりも小さければ、それらを先に中継する。その後の TCP 中継処理、および IPsec 関連の処理は既に述べた手順に準ずる。

【 0 0 9 1 】

次に、端末 1 0 2 が IPsec の機能を持たない IP 端末で、ルータ 7 0 1 がセキュリティサービスとして、ネットワーク 1 0 2 からネットワーク 2 0 1 へ出る、IPsec で保護されていないパケットを、IPsec のトンネルモードで保護する場合について述べる。特に、カプセル化されたパケットをプロキシーで扱う方法について説明する。Mobile IP など他のカプセル化の場合にも適用できる。

【 0 0 9 2 】

端末 1 0 2 と移動端末 5 0 2 の間の通信を想定する。移動端末 5 0 2 は、図 4 に構成を示すような IPsec 機能を持つ端末である。端末 1 0 2 は、図 7 に示すような構成であり IPsec 機能を持たない端末である。この間で通信を行う際に、図

8に構成を示すルータ701と移動端末502の間でIPSecを利用した通信を行う。このため、既に述べたものと同様な方式で、ルータ701と移動端末502の間のIPSec SAが確立され、更にセキュリティサーバ601を介して、プロキシ一介在を許容するIPSec SAの情報が必要なTCP-GW401に提供される。この際には、IPSecのトンネルモードが用いられる。端末102と移動端末502の間のパケットに対応するIPSecパケットは、図9(a)に示す形になる。

【0093】

TCP-GW401での中継処理は既に述べた方法に準ずる。但し、セキュリティ情報管理1424の制御の下でIPSecを解いてカプセル化も外した後のパケットについては、IP入力部1423がTCP中継を行うか否かを判断し、必要な場合にTCP1401にパケットを渡すことになる。また、パケットを送信する際はIPSecとカプセル化の処理を行う(図9(b)参照)。既に述べた方式との処理の切り替えは、SADから得たIPSec SA情報に含まれるIPSecプロトコルモードの値が、トランスポートモードであるか、トンネルモードであるかによって行うことができる。また、新しいIPヘッダが、カプセル化ヘッダであることを認識して行うこともできる。これは、例えばMobile IP(IETF RFC2002)によるHome AgentとForeign Agentの間のカプセル化されたTCP/IPパケットを扱うTCP-GWの場合など、一般にトンネルの中間にあるプロキシの場合にも適用できる。

【0094】

なお、上記の実施の形態はその主旨を逸脱しない範囲で種々変形して実施できることは言うまでもない。例えば、IPv6に適用することも可能である。

【0095】

また、有線端末と無線端末の間だけではなく、無線端末501と無線端末508の間の通信にも本発明が適用できることは明らかである。

【0096】

【発明の効果】

以上述べたような本発明によれば、IPSecなどでセキュリティを保証した通信に対しても、TCP-GWやSnoopに代表されるプロキシを適用して無線環境下での性能の向上を図ることができる。

【図面の簡単な説明】

【図 1】 本発明の中継装置、通信装置、制御装置を含んだネットワーク構成図。

【図 2】 本発明の TCP-GW のブロック構成図。

【図 3】 本発明の端末のブロック構成図。

【図 4】 本発明の移動端末のブロック構成図。

【図 5】 本発明のセキュリティサーバのブロック構成図。

【図 6】 本発明の IPSec 処理前後のパケットフォーマットの構成図。

【図 7】 本発明の別の端末のブロック構成図。

【図 8】 本発明のルータのブロック構成図。

【図 9】 本発明の IPSec 処理前後のパケットフォーマットの構成図。

【符号の説明】

101、102、103 端末

201、202、203、204 ネットワーク

301、302、303、304、305、306 基地局

401、402、403 TCP-GW

501、502、503、504、505、506、507、508 移動端末

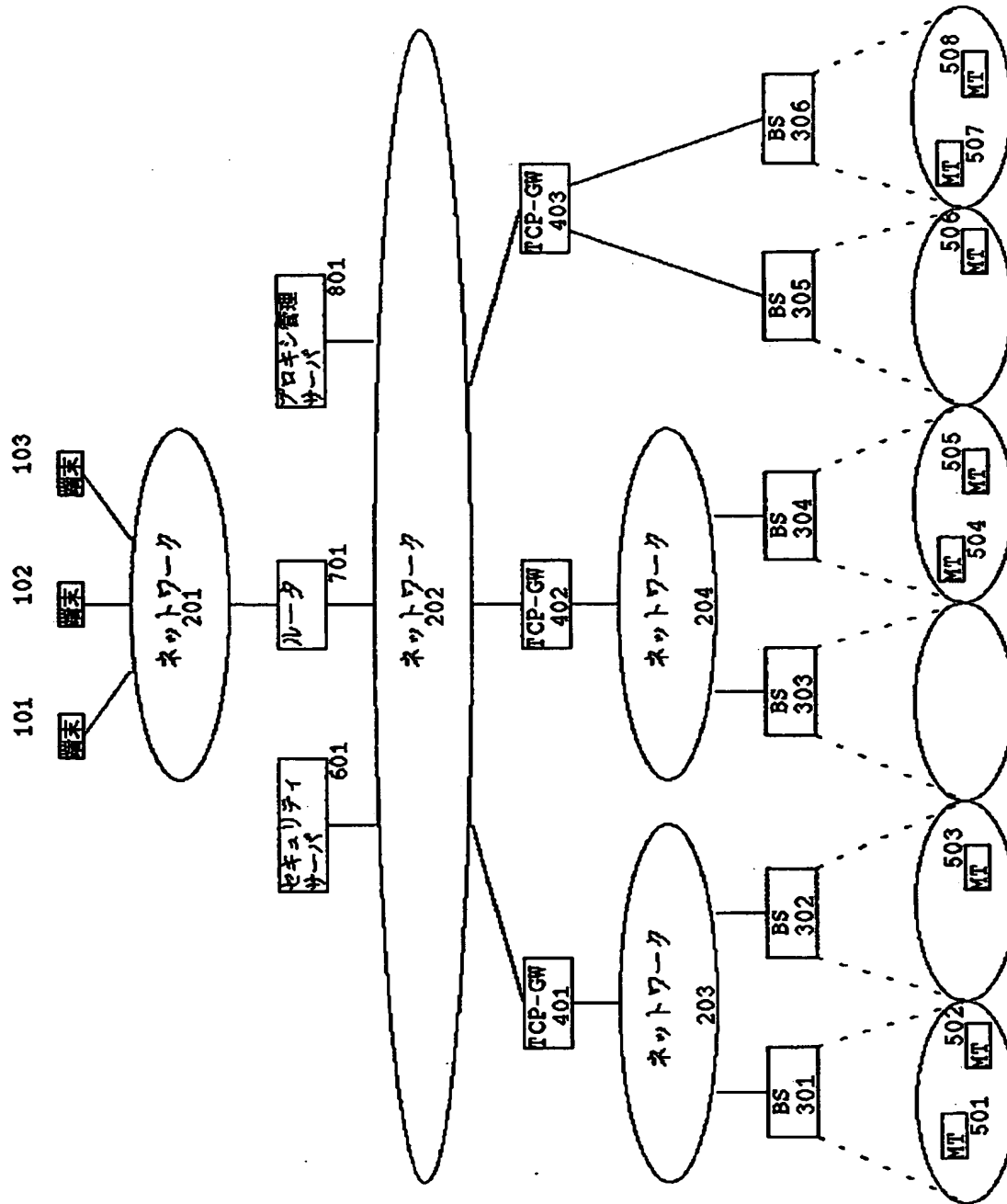
601 セキュリティサーバ

701 ルータ

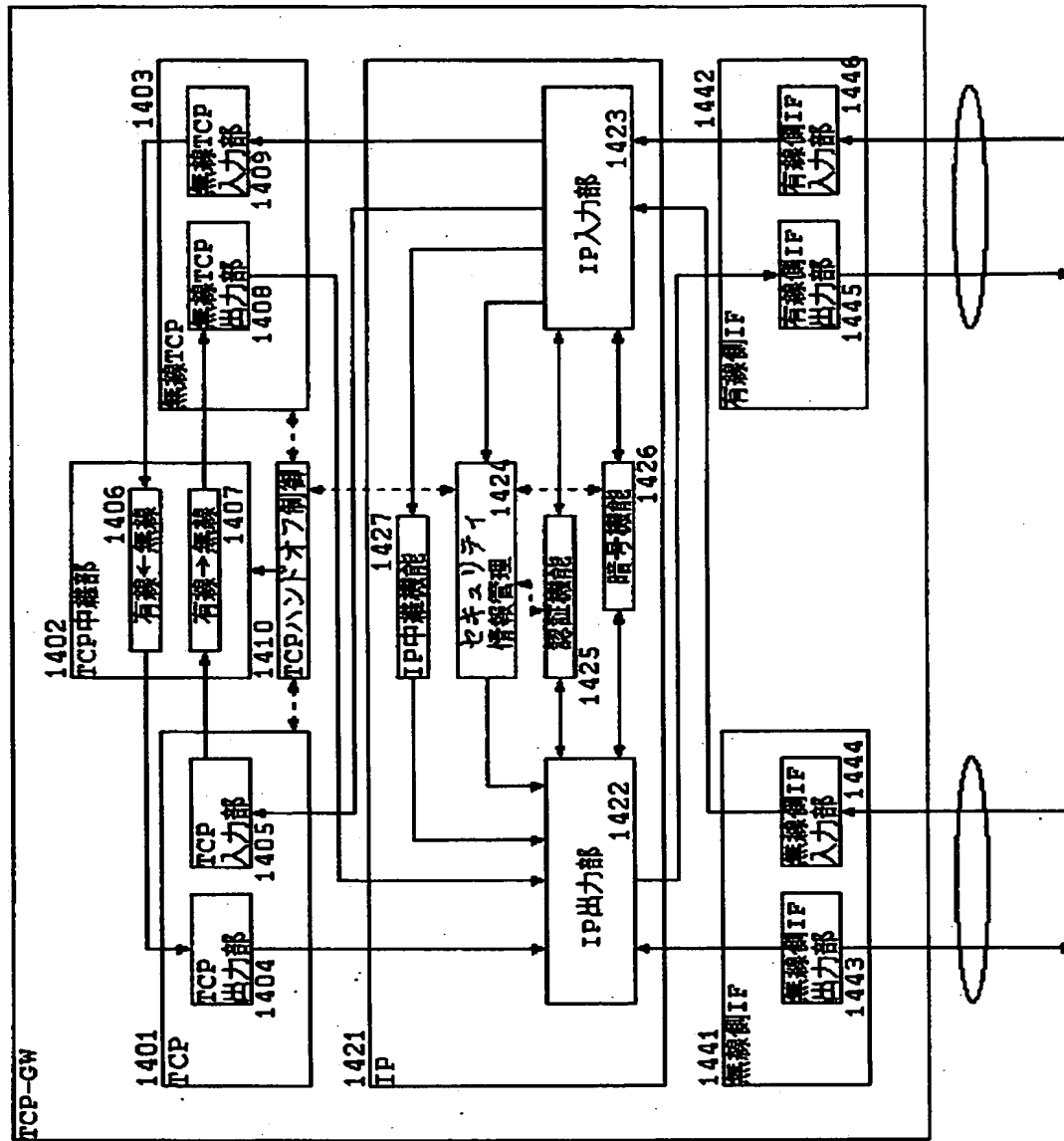
801 プロキシ管理サーバ

【書類名】 図面

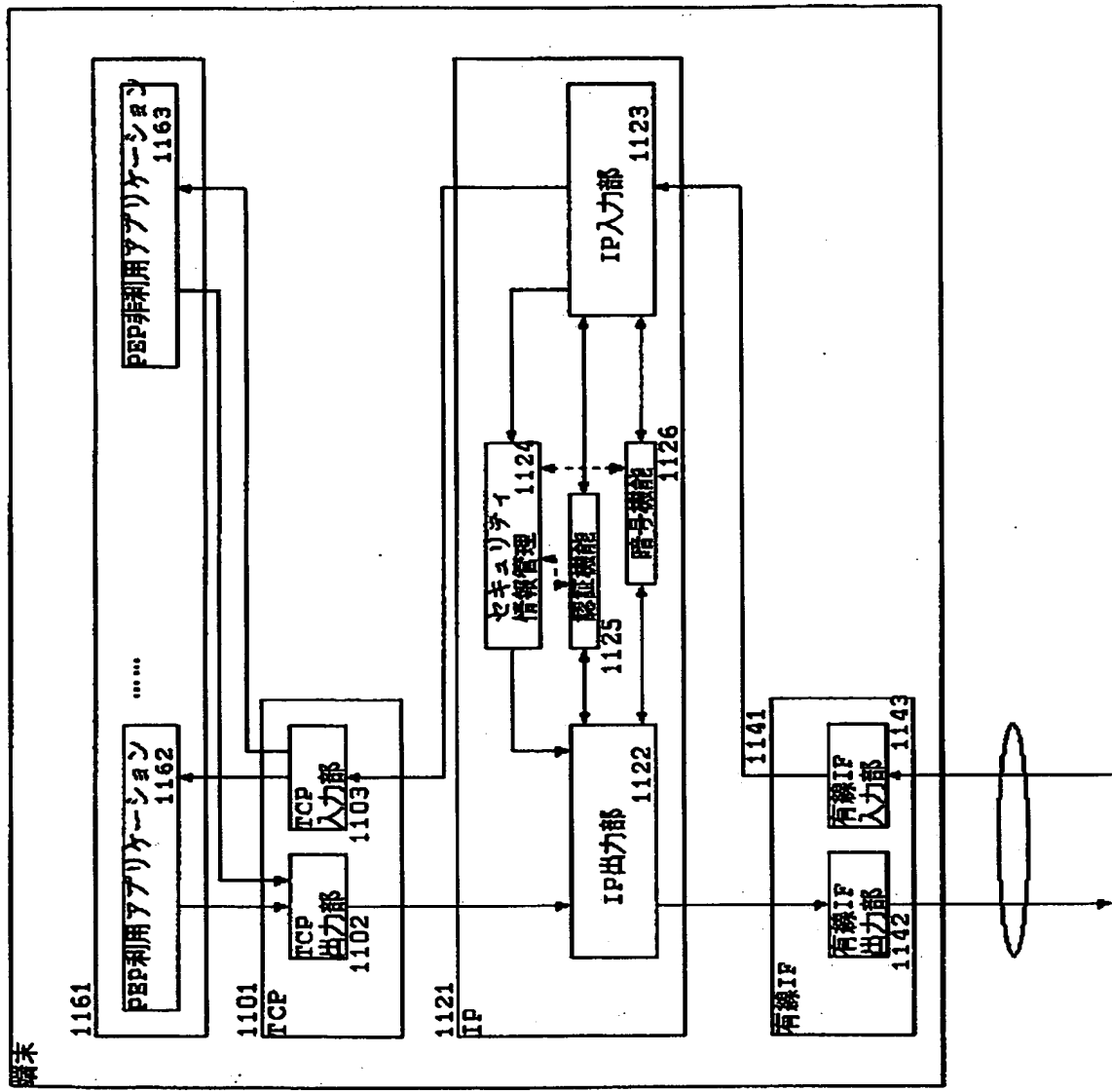
【図 1】



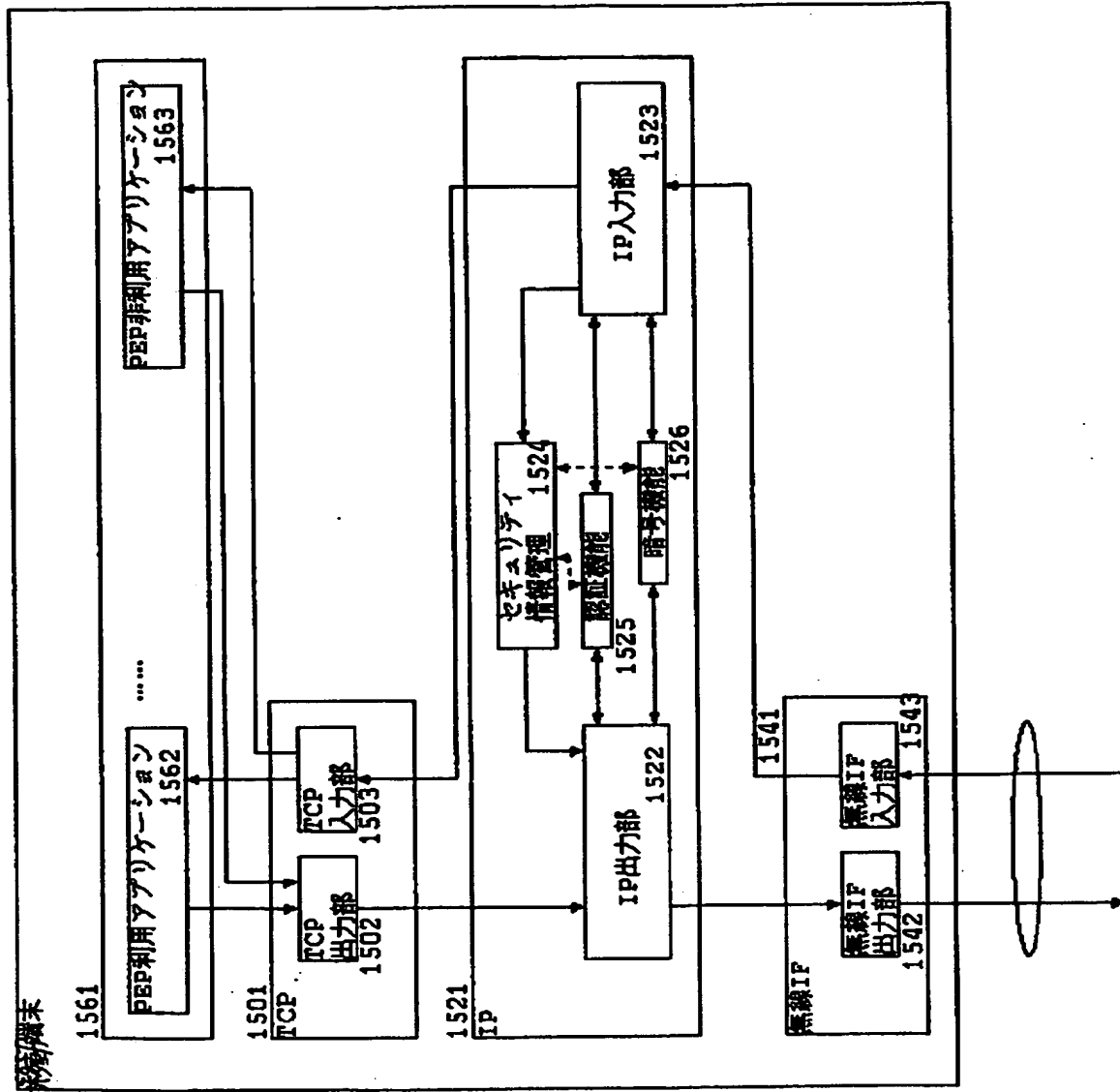
【図 2】



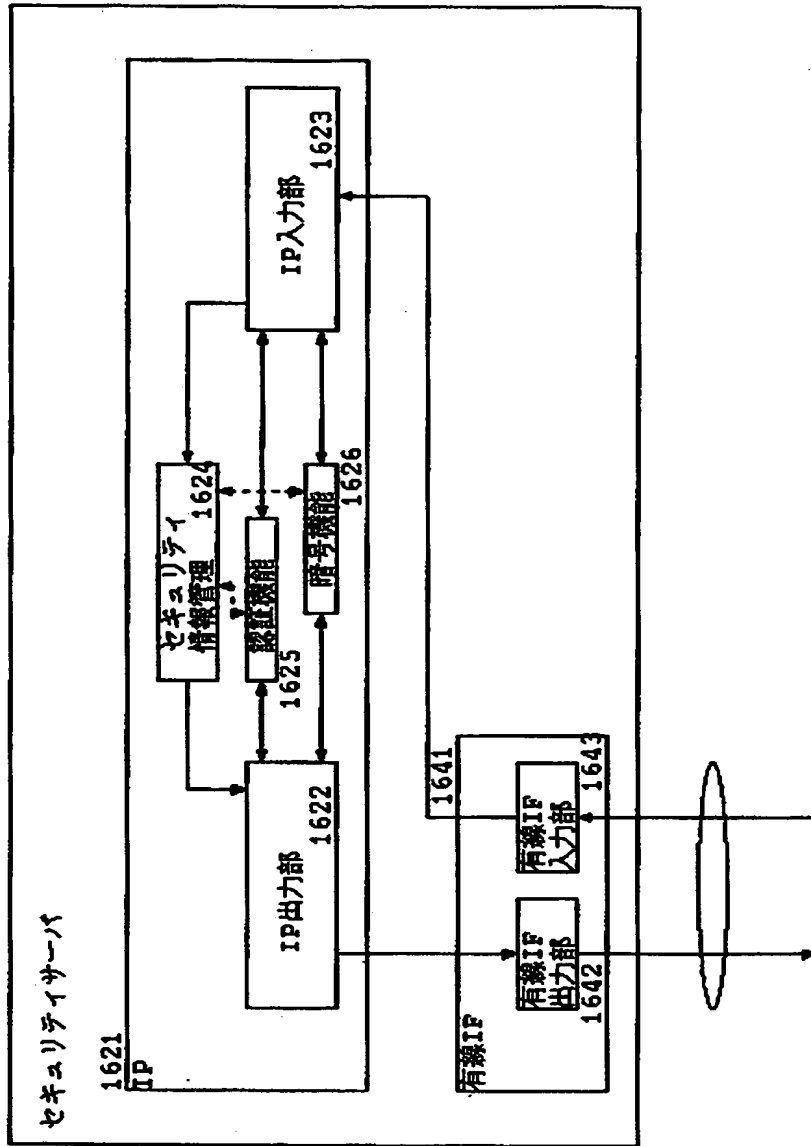
【図 3】



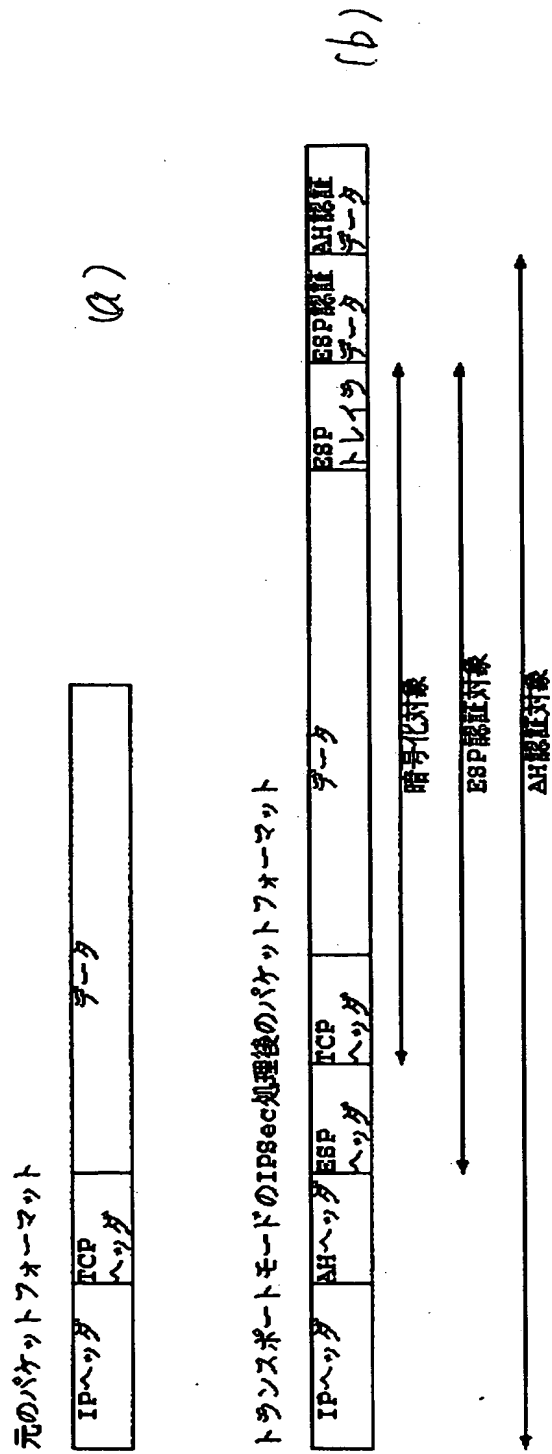
【図 4】



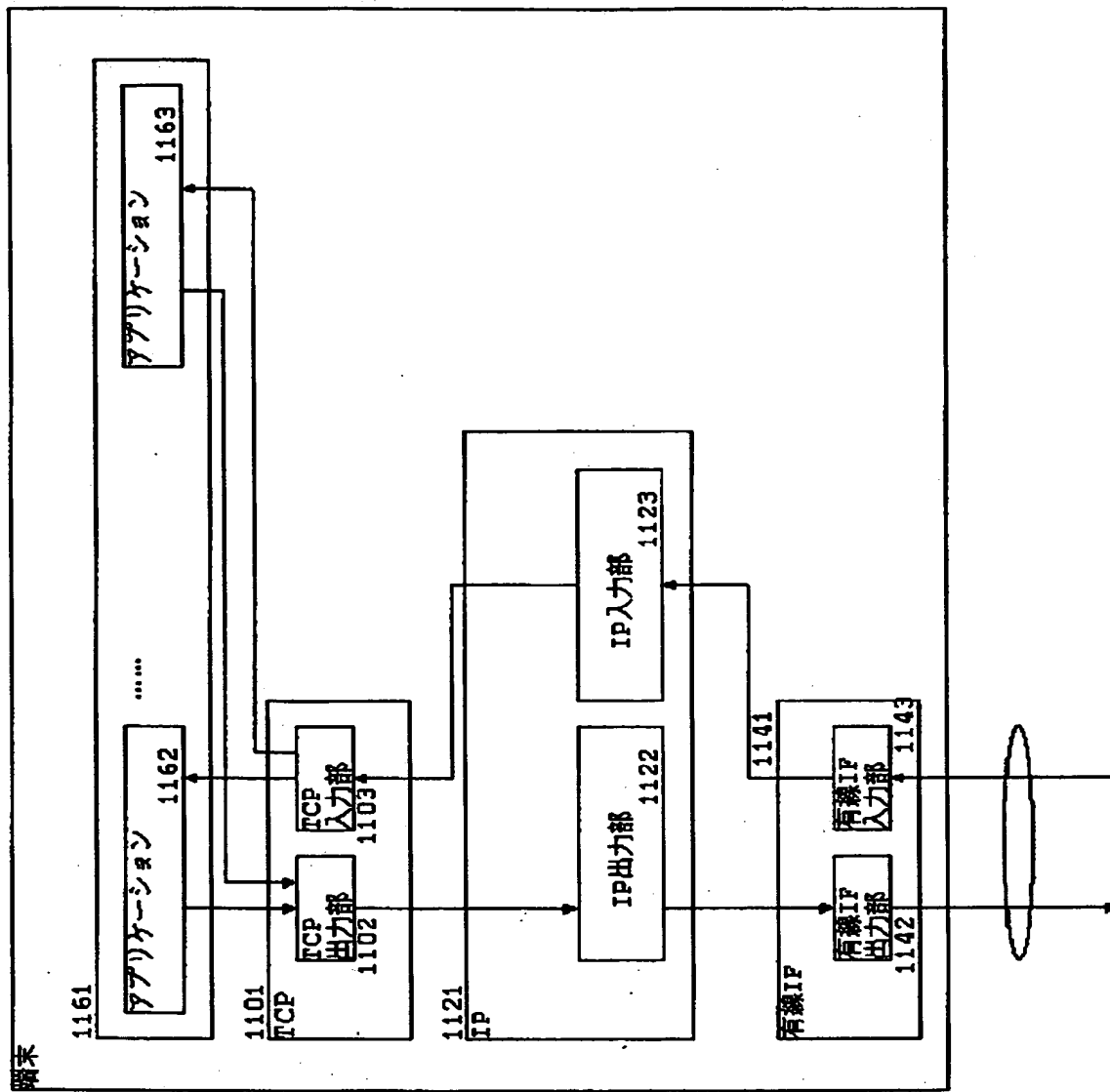
【図 5】



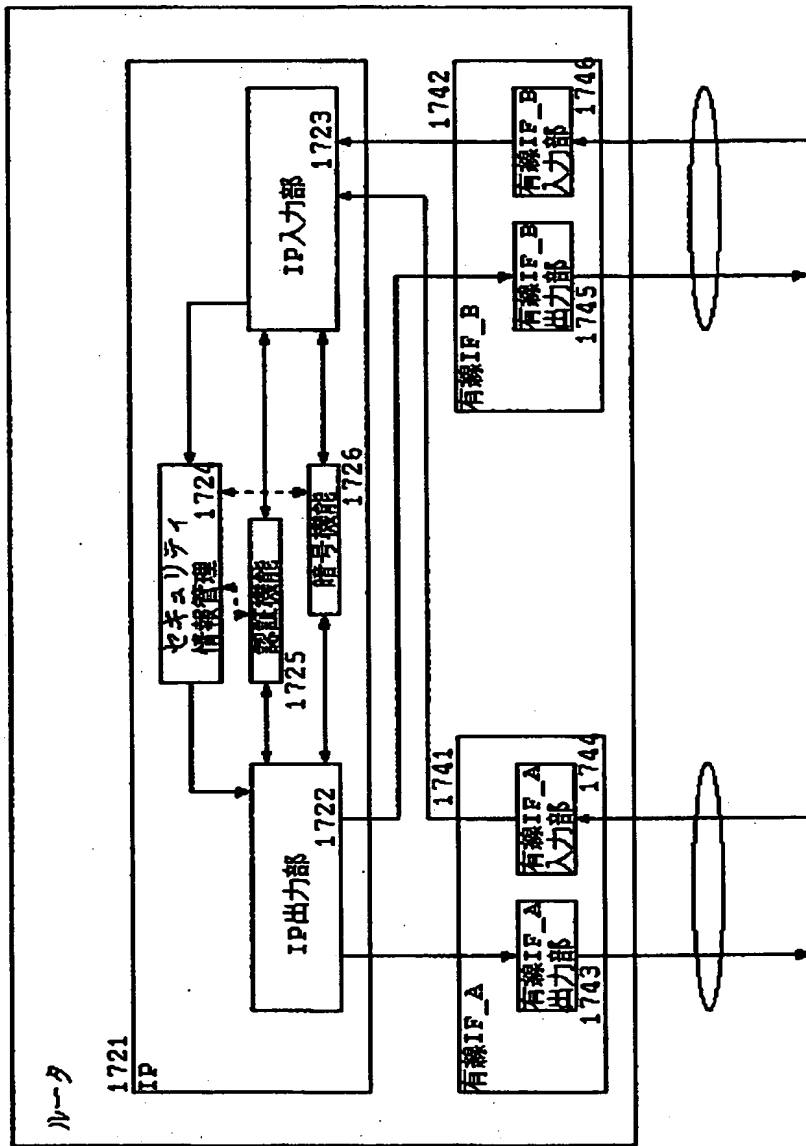
【図 6】



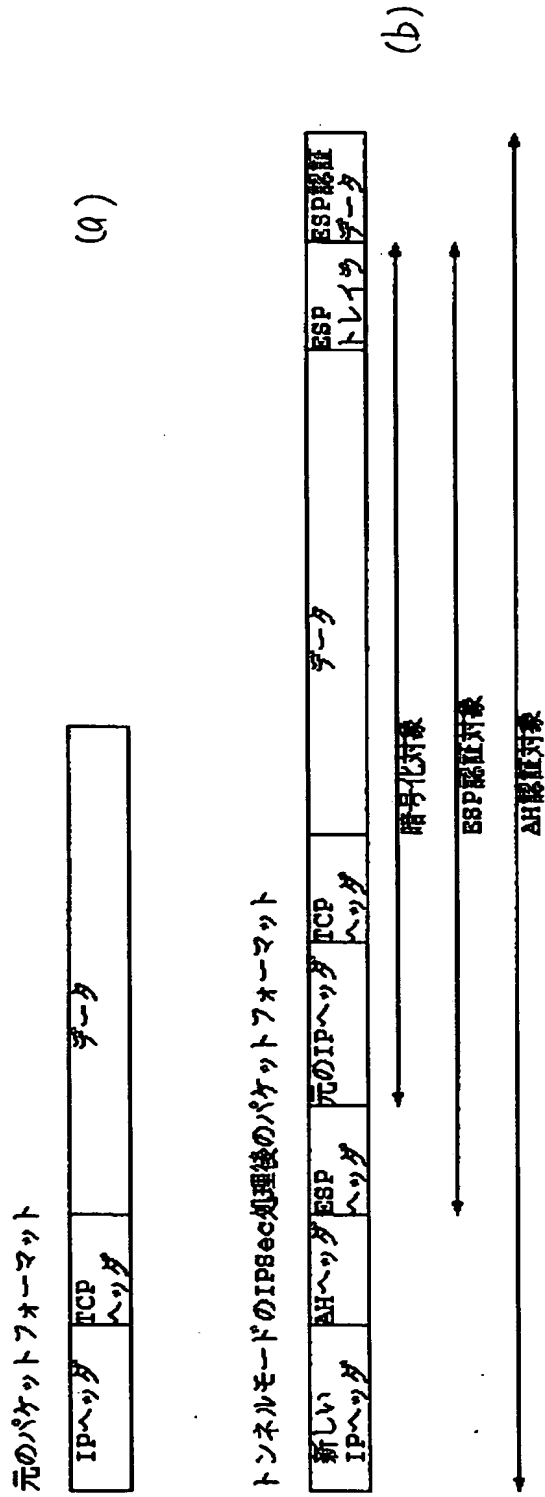
【図 7】



【図 8】



【図9】



【書類名】 要約書

【要約】

【課題】 セキュリティを維持しつつ、無線端末装置と有線端末装置間で通信を行う中継装置、通信装置、制御装置および通信制御方法の提供。

【解決手段】 ネットワーク 2 0 1 は TCP/IP 端末 1 0 1 ~ 1 0 3 を収容し、IP パケットを交換するルータ 7 0 1 によってネットワーク 2 0 2 と相互接続される。ネットワーク 2 0 2 は TCP-GW 4 0 1 と 4 0 2 とによってネットワーク 2 0 3、2 0 4 を、TCP-GW 4 0 3 によって基地局 3 0 5 と 3 0 6 を収容する。ネットワーク 2 0 2 はセキュリティサーバ 6 0 1 を持つ。ネットワーク 2 0 3 と 2 0 4 は、それぞれ基地局 3 0 1 と 3 0 2、基地局 3 0 3 と 3 0 4 を収容する。基地局 3 0 1 には移動端末 5 0 1 と 5 0 2、基地局 3 0 2 には移動端末 5 0 3、基地局 3 0 4 には移動端末 5 0 4 と 5 0 5、基地局 3 0 5 には移動端末 5 0 6、そして基地局 3 0 6 には移動端末 5 0 7 と 5 0 8 が存在する。移動端末 5 0 1 ~ 5 0 8 は TCP/IP 端末である。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日	1990年 8月22日
[変更理由]	新規登録
住 所	神奈川県川崎市幸区堀川町72番地
氏 名	株式会社東芝